# SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203

## DEPARTMENT OF CYBER SECURITY

## QUESTION BANK

**VI SEMESTER**

**CY3663-DIGITAL FORENSICS**

**Regulation – 2023**

**Academic Year 2025 – 26 (Even Semester)**

*Prepared by*

**Ms. M. RAGHAVI, Assistant Professor (O.G)/CYS**

# SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

**DEPARTMENT OF CYBER SECURITY**

**QUESTION BANK**

**SUBJECT CODE & NAME: CY3663-DIGITAL FORENSICS**

**SEM / YEAR: VI Sem/ III Year**

| UNIT I – INTRODUCTION TO DIGITAL FORENSIC | | | |
|---|---|---|---|
| Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase | | | |
| **PART A** | | | |
| **Q. No** | **Questions** | **BT Level** | **Competence** |
| 1. | Define Digital Forensics and explain its primary objective in investigations. | BTL-1 | Remembering |
| 2. | What is Digital Evidence, and why is it considered highly sensitive in cyber investigations? | BTL-1 | Remembering |
| 3. | List and briefly describe the major phases involved in the Digital Forensics Process. | BTL-2 | Understanding |
| 4. | What is meant by Chain of Custody, and why is it essential for maintaining evidence validity? | BTL-2 | Understanding |
| 5. | Differentiate between live data and static data with suitable examples. | BTL-2 | Understanding |
| 6. | What is a forensic image, and how does it differ from a normal data copy? | BTL-1 | Remembering |
| 7. | Describe the purpose of the Identification phase in the forensic investigation process. | BTL-2 | Understanding |
| 8. | What is volatile digital evidence? Give an example. | BTL-1 | Remembering |
| 9. | State the role of the Collection phase and why accuracy is critical during evidence gathering. | BTL-2 | Understanding |
| 10. | Define acquisition in digital forensics and state its importance. | BTL-1 | Remembering |
| 11. | What is a forensic toolkit, and why is tool selection important for investigators? | BTL-2 | Understanding |
| 12. | What is time-stamping, and how is it used in forensic analysis? | BTL-2 | Understanding |
| 13. | Define data preservation and describe its significance in digital forensics. | BTL-2 | Understanding |
| 14. | What is a Digital Forensic Process Model? Provide an example. | BTL-1 | Remembering |
| 15. | Explain what evidence admissibility means in the context of cyber law. | BTL-2 | Understanding |
| 16. | What is bit-stream imaging, and when is it used in forensics? | BTL-1 | Remembering |
| 17. | Define file carving and explain where it is used in investigations. | BTL-2 | Understanding |
| 18. | What is write protection, and how does it prevent evidence alteration? | BTL-1 | Remembering |
| 19. | Define forensic reporting and mention its key components. | BTL-2 | Understanding |
| 20. | What is metadata, and how does it aid investigators? | BTL-2 | Understanding |

| | | | |
|---|---|---|---|
| 21. | List any two major challenges encountered in digital forensic investigations. | BTL-2 | Understanding |
| 22. | What is evidence integrity, and how is it verified? | BTL-2 | Understanding |
| | **PART - B** | | |
| 1. | Explain in detail every phase of the Digital Forensics Process with neat diagrams and real-time examples. (16) | BTL-2 | Understanding |
| 2. | Discuss the various types of Digital Evidence, highlighting their characteristics and challenges in handling. (16) | BTL-2 | Understanding |
| 3. | Describe the role of Identification, Collection, Examination, and Analysis phases in a forensic investigation. (16) | BTL-3 | Applying |
| 4. | Explain the structure, purpose, and legal importance of the Chain of Custody in digital forensics. (16) | BTL-4 | Analyzing |
| 5. | Discuss the operational and technical challenges faced while handling digital evidence from modern devices (16) | BTL-4 | Analyzing |
| 6. | Describe in detail the various forensic imaging techniques and compare tools such as FTK Imager, EnCase, and dd. (16) | BTL-3 | Applying |
| 7. | Explain the steps involved in forensic documentation and report preparation with a sample format. (16) | BTL-3 | Applying |
| 8. | Illustrate the workflow for evidence acquisition, storage, and preservation ensuring non-tampering. (16) | BTL-3 | Applying |
| 9. | Compare traditional physical forensics and digital forensics with examples. (16) | BTL-4 | Analyzing |
| 10. | Explain the features of admissible digital evidence and the requirements for presenting it in court. (16) | BTL-4 | Analyzing |
| 11. | Discuss hashing algorithms (MD5, SHA-1, SHA-256) and their role in maintaining digital integrity. (16) | BTL-4 | Analyzing |
| 12. | Explain forensic examination techniques such as keyword searching, log analysis, and timeline reconstruction. (16) | BTL-3 | Applying |
| 13. | Describe file system analysis, deleted file recovery, and hidden data retrieval methods. (16) | BTL-3 | Applying |
| 14. | Explain different digital forensic models such as DFRWS, NIST, and Integrated DF Model. (16) | BTL-2 | Understanding |
| 15. | Discuss the responsibilities, ethics, and legal obligations of digital forensic investigators. (16) | BTL-4 | Analyzing |
| 16. | Explain the steps involved in preparing, validating, and presenting digital evidence before a judge or jury. (16) | BTL-5 | Evaluating |
| 17. | Discuss the latest challenges and limitations in digital forensics such as encryption, large-scale storage, and cloud technology. (16) | BTL-5 | Evaluating |
| | | | |
| | **UNIT II – DIGITAL CRIME AND INVESTIGATION** | | |
| | Digital Crime – Substantive Criminal Law – General Conditions – Offenses – Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence | | |
| | **PART – A** | | |
| 1. | Define Digital Crime and explain how it differs from traditional crime. | BTL-1 | Remembering |
| 2. | What is cyber jurisdiction, and why does it complicate international investigations? | BTL-2 | Understanding |
| 3. | What is cyber fraud? Provide an example of a commonly reported case. | BTL-1 | Remembering |
| 4. | List two major categories of cyber offenses under ICT laws. | BTL-2 | Understanding |

| | | | |
|---|---|---|---|
| 5. | What is cyber terrorism, and how does it threaten national security? | BTL-1 | Remembering |
| 6. | Define cyber stalking and mention one commonly used method. | BTL-1 | Remembering |
| 7. | What is malware forensics, and what type of malware typically requires forensic study? | BTL-2 | Understanding |
| 8. | Define a digital crime scene and describe its importance. | BTL-2 | Understanding |
| 9. | Define substantive criminal law and explain its relevance in cybercrime penalties. | BTL-2 | Understanding |
| 10. | What are MLATs, and how do they support cross-border cybercrime investigations? | BTL-2 | Understanding |
| 11. | What is a digital search warrant, and when is it required? | BTL-2 | Understanding |
| 12. | What is cross-border cyber investigation? Provide an example. | BTL-2 | Understanding |
| 13. | Define digital intelligence and list one technique used to collect it. | BTL-2 | Understanding |
| 14. | Provide any two common examples of cybercrime investigated today. | BTL-1 | Remembering |
| 15. | What is IP address tracing in cybercrime investigation? | BTL-2 | Understanding |
| 16. | Define cyber intrusion and provide an example scenario. | BTL-2 | Remembering |
| 17. | What is forensic triage, and why is it used at crime scenes? | BTL-3 | Applying |
| 18. | What is chain-of-events reconstruction in forensic investigation? | BTL-3 | Applying |
| 19. | What is digital surveillance, and how is it regulated? | BTL-2 | Understanding |
| 20. | What is email spoofing, and why is it dangerous? | BTL-2 | Understanding |
| 21. | What is cyber extortion? Provide an example. | BTL-2 | Understanding |
| 22. | What is evidence collection, and why must it follow protocol? | BTL-2 | Understanding |
| | **PART – B** | | |
| 1. | Discuss the major categories of digital crimes with detailed real-time examples. (16) | BTL-2 | Understanding |
| 2. | Explain the legal aspects of cybercrime investigation under various criminal laws and acts. (16) | BTL-2 | Understanding |
| 3. | Describe in detail the investigation methods used to collect and analyze digital evidence. (16) | BTL-3 | Applying |
| 4. | Explain international cooperation models, treaties, and agreements used in cross-border cybercrime investigations. (16) | BTL-4 | Analyzing |
| 5. | Describe the role of law enforcement agencies (LEA) in handling digital crime cases. (16) | BTL-4 | Analyzing |
| 6. | Compare traditional crime investigation with modern digital crime investigation methods. (16) | BTL-4 | Analyzing |
| 7. | Explain the full workflow of digital crime investigation from complaint to charge-sheet. (16) | BTL-3 | Applying |
| 8. | Discuss the forensic techniques used in IP tracing, log analysis, and network forensics. (16) | BTL-4 | Analyzing |
| 9. | Explain cyber fraud, types of frauds, and detailed steps of fraud investigation. (16) | BTL-4 | Analyzing |
| 10. | Discuss challenges faced in global cybercrime investigations such as anonymity, VPNs, and dark web. (16) | BTL-5 | Evaluating |

| | | | |
|---|---|---|---|
| 11. | Describe the steps investigators follow when approaching a digital crime scene. (16) | BTL-3 | Applying |
| 12. | Explain cyber terrorism and methods used to track cyber-terrorist activities. (16) | BTL-4 | Analyzing |
| 13. | Discuss forensic case reconstruction using logs, timestamps, and metadata correlation. (16) | BTL-4 | Analyzing |
| 14. | Describe malware analysis techniques such as static, dynamic, and hybrid analysis. (16) | BTL-4 | Analyzing |
| 15. | Explain cyber laws (IT Act, GDPR, etc.) and their impact on digital forensic practices. (16) | BTL-5 | Evaluating |
| 16. | Discuss cloud-based cybercrime investigations and issues in collecting cloud evidence. (16) | BTL-5 | Evaluating |
| 17. | Explain the importance of digital intelligence in modern policing. (16) | BTL-5 | Evaluating |

**UNIT III – DIGITAL FORENSIC READINESS**

Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Enterprise Digital Forensic Readiness – Challenges in Digital Forensics

**PART - A**

| | | | |
|---|---|---|---|
| 1. | Define Digital Forensic Readiness and explain why organizations need to implement it. | BTL-1 | Remembering |
| 2. | What is a forensic readiness plan, and what purpose does it serve in investigation preparedness? | BTL-2 | Understanding |
| 3. | Define proactive forensics and state one situation where it is applied. | BTL-1 | Remembering |
| 4. | What is enterprise forensic readiness, and how does it support incident response activities? | BTL-2 | Remembering |
| 5. | What is evidence retention, and why must organizations follow strict retention schedules? | BTL-2 | Understanding |
| 6. | What is log correlation, and how does it help investigators identify suspicious activity? | BTL-3 | Applying |
| 7. | Mention any two international standards related to forensic readiness. | BTL-1 | Remembering |
| 8. | What is ISO/IEC 27043, and what does it define in the context of digital Forensics? | BTL-2 | Understanding |
| 9. | What is meant by readiness maturity in forensic operations? | BTL-2 | Understanding |
| 10. | Define incident response and state its role in forensic readiness. | BTL-2 | Understanding |
| 11. | What is continuous monitoring, and why is it important for early detection of threats? | BTL-1 | Remembering |
| 12. | Define audit logging and explain its role in forensic investigations. | BTL-2 | Understanding |
| 13. | What are forensic policies, and why must companies implement them? | BTL-2 | Understanding |
| 14. | What is an evidence preservation strategy? | BTL-1 | Remembering |
| 15. | Define digital preparedness and mention one of its essential components. | BTL-2 | Understanding |
| 16. | What is event reconstruction in digital forensic investigations? | BTL-3 | Applying |
| 17. | Mention one major challenge faced by organizations while establishing forensic readiness. | BTL-1 | Remembering |
| 18. | What is threat intelligence, and how is it useful in forensic operations? | BTL-2 | Understanding |

| | | | |
|---|---|---|---|
| 19. | What is SIEM, and how does it assist in digital forensic readiness? | BTL-2 | Understanding |
| 20. | Define alert generation and give one example of an alert that helps investigations. | BTL-1 | Remembering |
| 21. | What is data leakage detection in an enterprise environment? | BTL-1 | Remembering |
| 22. | What are readiness controls, and how do they support proactive forensic activity? | BTL-3 | Applying |
| | **PART - B** | | |
| 1. | Explain in detail the concept, need, benefits, and complete process of Digital Forensic Readiness in an organization. (16) | BTL-2 | Understanding |
| 2. | Compare law enforcement forensic readiness with enterprise forensic readiness, discussing objectives, procedures, and scope. (16) | BTL-4 | Analyzing |
| 3. | Discuss international frameworks and standards such as ISO 27043, NIST guidelines, and ACPO principles for forensic readiness. (16) | BTL-5 | Evaluating |
| 4. | Explain how forensic readiness supports and enhances the overall incident response strategy for modern organizations. (16) | BTL-4 | Analyzing |
| 5. | Describe the step-by-step procedures involved in implementing enterprise forensic readiness with suitable examples. (16) | BTL-3 | Applying |
| 6. | Discuss the legal, operational, and technical challenges faced while establishing forensic readiness across different environments. (16) | BTL-4 | Analyzing |
| 7. | Explain the importance of logging, monitoring, and auditing systems in ensuring strong forensic readiness. (16) | BTL-3 | Applying |
| 8. | Describe the processes involved in digital evidence retention, secure storage, retrieval, and policy considerations. (16) | BTL-5 | Evaluating |
| 9. | Discuss the role, architecture, and importance of SIEM tools in digital forensic readiness. (16) | BTL-4 | Analyzing |
| 10. | Explain how digital forensic readiness improves the ability of organizations to respond to cyber threats and attacks. (16) | BTL-4 | Analyzing |
| 11. | Describe the key technical components required to achieve effective forensic readiness in cloud-based environments. (16) | BTL-3 | Applying |
| 12. | Explain evidence collection, documentation, and preservation procedures within a forensic readiness program. (16) | BTL-3 | Applying |
| 13. | Discuss how organizations can design and test a forensic readiness policy and strategy for improved cyber resilience. (16) | BTL-4 | Analyzing |
| 14. | Explain the importance of risk assessment and how it influences readiness planning in digital forensics. (16) | BTL-3 | Applying |
| 15. | Describe the structure and purpose of proactive monitoring systems and how they help in early forensic detection. (16) | BTL-3 | Applying |
| 16. | Discuss various tools and techniques used to support digital forensic readiness with suitable use case examples. (16) | BTL-4 | Analyzing |
| 17. | Explain the overall role of forensic readiness in strengthening organizational cybersecurity and incident management. (16) | BTL-5 | Evaluating |
| | | | |

| UNIT IV – PROCESSING DIGITAL CRIME SCENES AND SECURING EVIDENCE | | | |
|---|---|---|---|
| Overview of Digital Crime Scene Processing – Securing a Computer Incident or Crime Scene – Seizing Digital Evidence at the Scene – Storing Digital Evidence – Obtaining Digital Hashes – Reviewing the Case and Evidence – Evidence Documentation and Chain of Custody – Case Management and Collaboration – Legal and Ethical Considerations | | | |
| **PART – A** | | | |
| 1. | Define a digital crime scene and explain why it is treated differently from a physical crime scene. | BTL-1 | Remembering |
| 2. | What is the role of a first responder in a digital forensic investigation? | BTL-1 | Remembering |
| 3. | Define volatile digital evidence and give an example of where it can be found. | BTL-1 | Remembering |
| 4. | Define non-volatile evidence and explain its significance in investigations. | BTL-1 | Remembering |
| 5. | What is a write blocker, and how does it prevent alteration of digital evidence? | BTL-1 | Remembering |
| 6. | Define logical acquisition and describe its purpose in forensic examinations. | BTL-2 | Understanding |
| 7. | What is forensic duplication, and why is it necessary before analysis? | BTL-2 | Understanding |
| 8. | Explain forensic imaging and how it is used to preserve evidence. | BTL-2 | Understanding |
| 9. | What is evidence preservation, and why must it be done carefully at a crime scene? | BTL-2 | Understanding |
| 10. | What is a chain-of-custody form, and what details are recorded on it? | BTL-2 | Understanding |
| 11. | What is case documentation, and why is it critical in digital investigations? | BTL-2 | Understanding |
| 12. | Define evidence bagging and labeling in forensic practice. | BTL-2 | Understanding |
| 13. | What is hashing, and how is it used to verify integrity of digital evidence? | BTL-2 | Understanding |
| 14. | What is on-site analysis, and when is it performed? | BTL-2 | Understanding |
| 15. | Define evidence review and its role before presenting in court. | BTL-2 | Understanding |
| 16. | What is incident isolation, and why is it important in a digital crime scene? | BTL-2 | Understanding |
| 17. | What is tamper-proof storage, and how does it protect digital evidence? | BTL-2 | Understanding |
| 18. | Define case management in digital forensic investigations. | BTL-2 | Understanding |
| 19. | What is triage analysis, and how does it help prioritize evidence processing? | BTL-3 | Applying |
| 20. | Define forensic preview and its purpose in initial examination. | BTL-3 | Applying |
| 21. | What is anti-contamination procedure, and why is it necessary at crime | BTL-3 | Applying |

| | | | |
|---|---|---|---|
| | scenes? | | |
| 22. | What is an acquisition log, and what information does it record? | BTL-3 | Applying |
| | **PART - B** | | |
| 1. | Explain the complete process of digital crime scene processing, including all steps from arrival to documentation, with diagrams. (16) | BTL-3 | Applying |
| 2. | Describe in detail the procedures for seizing digital evidence at a crime scene, including hardware, software, and network devices. | BTL-3 | Applying |
| 3. | Explain various methods for storing and protecting digital evidence during transportation and lab analysis. (16) | BTL-3 | Applying |
| 4. | Discuss the process of obtaining digital hashes and explain their importance in validating evidence integrity. (16) | BTL-4 | Analyzing |
| 5. | Describe the procedures for proper documentation and maintaining chain-of-custody forms. (16) | BTL-3 | Applying |
| 6. | Explain case management and collaborative tools used in digital forensic investigations. (16) | BTL-3 | Applying |
| 7. | Discuss legal and ethical considerations when handling digital evidence at crime scenes. (16) | BTL-4 | Analyzing |
| 8. | Describe methods of collecting both volatile and non-volatile data during on-site forensic analysis. (16) | BTL-3 | Applying |
| 9. | Explain the use of write blockers and imaging tools in preserving evidence without altering original data. (16) | BTL-3 | Applying |
| 10. | Discuss common mistakes made at digital crime scenes and how they can compromise investigations. (16) | BTL-4 | Understanding |
| 11. | Explain the workflow of incident response in digital crime scenes, including triage and evidence prioritization. (16) | BTL-3 | Applying |
| 12. | Describe off-site investigation procedures, including transporting and storing digital evidence securely. (16) | BTL-3 | Analyzing |
| 13. | Explain the process of evidence verification and validation in forensic laboratories. (16) | BTL-4 | Analyzing |
| 14. | Discuss challenges faced when handling encrypted, password-protected, or cloud-based evidence. (16) | BTL-4 | Analyzing |
| 15. | Explain standards and procedures for tamper-proof storage of digital evidence in forensic labs. (16) | BTL-4 | Analyzing |
| 16. | Describe legal search and seizure requirements specific to digital crime scenes. (16) | BTL-4 | Analyzing |
| 17. | Explain how forensic investigators review cases and prepare evidence for courtroom presentation. (16) | BTL-5 | Evaluating |
| | **UNIT V – ADVANCED COMPUTER FORENSICS TOOLS AND TECHNIQUES** | | |

| | | | |
|---|---|---|---|
| Introduction to Computer Forensics Tools – Validating and Testing Forensic Software – Addressing Data-Hiding Techniques – Performing Remote Acquisitions – Email Investigations: Investigating Email Crime and Violations – Understanding Email Servers – Specialized Email Forensics Tools – Digital Forensics in Legal Context – Ethical Considerations in Email Investigations. | | | |
| **PART – A** | | | |
| 1. | Define forensic tools and explain why selecting the correct tool is important for investigations. | BTL-1 | Remembering |
| 2. | What is remote acquisition, and when is it necessary to use it? | BTL-2 | Understanding |
| 3. | Define steganography and explain how it can hide digital evidence. | BTL-2 | Understanding |
| 4. | Define anti-forensics and give an example of a technique used to evade detection. | BTL-2 | Understanding |
| 5. | What is metadata, and how is it useful in forensic investigations? | BTL-2 | Understanding |
| 6. | What is an email header, and what information can investigators obtain from it? | BTL-2 | Understanding |
| 7. | Define forensic automation and explain its benefits in large-scale investigations. | BTL-3 | Applying |
| 8. | What is email spoofing, and why is it a threat in cyber investigations? | BTL-2 | Understanding |
| 9. | Define data carving and explain when it is used in forensic analysis. | BTL-3 | Remembering |
| 10. | Name two forensic imaging tools and their primary functions. | BTL-1 | Remembering |
| 11. | What is a log file, and how can it help in analyzing an incident? | BTL-2 | Understanding |
| 12. | What is a mail server, and why is understanding its structure important in email forensics? | BTL-2 | Understanding |
| 13. | Define email forensics and explain its role in investigating cyber crimes. | BTL-2 | Understanding |
| 14. | What is hashing, and how is it used to verify integrity in forensic analysis? | BTL-2 | Understanding |
| 15. | Explain what a Mail Transfer Agent (MTA) is and its relevance in email investigations. | BTL-2 | Understanding |
| 16. | What is a specialized email forensic tool, and give one example. | BTL-3 | Applying |
| 17. | Define cloud email forensics and its importance in modern investigations. | BTL-3 | Applying |
| 18. | What are data-hiding techniques, and how do they complicate forensic analysis? | BTL-2 | Understanding |
| 19. | What is log analysis in forensic investigations? | BTL-3 | Applying |
| 20. | Define forensic reporting in email and computer investigations. | BTL-3 | Applying |
| 21. | What is evidence acquisition from networked systems? | BTL-2 | Understanding |
| 22. | Explain how digital forensic tools support ethical and legal compliance in investigations. | BTL-3 | Applying |

| PART - B | | | |
|---|---|---|---|
| 1. | Explain the types of computer forensic tools and their applications in detail. (16) | BTL-3 | Applying |
| 2. | Discuss the validation and testing process for forensic software and why it is necessary. (16) | BTL-4 | Analyzing |
| 3. | Explain various data-hiding techniques, such as steganography and encryption, and how investigators detect them. (16) | BTL-5 | Evaluating |
| 4. | Describe procedures for performing remote acquisition of digital evidence and associated challenges. (16) | BTL-4 | Analyzing |
| 5. | Explain the process of email investigation, including header analysis, server logs, and forensic tools. (16) | BTL-3 | Applying |
| 6. | Compare different email servers and their forensic features. (16) | BTL-4 | Analyzing |
| 7. | Explain specialized email forensic tools and their usage in cybercrime investigation. (16) | BTL-3 | Applying |
| 8. | Discuss digital forensics in a legal context, including evidence presentation in court. (16) | BTL-5 | Evaluating |
| 9. | Examine ethical issues in computer and email forensic investigations with examples. (16) | BTL-4 | Analyzing |
| 10. | Explain forensic analysis of cloud-based email systems, including acquisition and verification. (16) | BTL-4 | Analyzing |
| 11. | Describe the workflow of advanced forensic tools used in large-scale enterprise investigations. (16) | BTL-4 | Analyzing |
| 12. | Discuss how anti-forensics techniques affect forensic investigations and ways to overcome them. (16) | BTL-4 | Analyzing |
| 13. | Explain forensic imaging of storage devices, including tools and procedures to prevent evidence alteration. (16) | BTL-4 | Analyzing |
| 14. | Evaluate the advantages and limitations of forensic automation tools in modern investigations. (16) | BTL-5 | Evaluating |
| 15. | Explain the role of hashing algorithms and validation in computer and email forensics. (16) | BTL-4 | Analyzing |
| 16. | Discuss email crime investigations with step-by-step methodology and tools used. (16) | BTL-5 | Evaluating |
| 17. | Explain how advanced digital forensic tools support cybercrime investigations and provide case-based examples. (16) | BTL-5 | Evaluating |